# Section 7

# Advanced Data Recovery and the Legal Profession

Tom Kapurch
Data Recovery Services, Inc
Dallas, Texas

# Advanced Data Recovery and the Legal Profession
# A Continuing Education Course

**TX MCLE Course # 000030851**

**Presented by**

**Data Recovery Services, Inc**

**Dallas, TX**

**Houston, TX**

**Washington, DC**

**Sydney, Australia**

# Advanced Data Recovery and the Legal Profession
# A Continuing Education Course

### TX MCLE Course # 000030851

### Outline

**Introduction** General relevance of data believed lost, damaged or destroyed.

I. Legal considerations in preparation for recovery
   - A. General Application
   - B. Evidentiary Application
     1. Protection and preservation of original evidence
     2. Imaging

II. Technical Background
   - A. How electronic data storage devices work
     1. Magnetic media
     2. CDs and CD ROMs
   - B. Symptoms, causes and types of data failure
     1. Mechanical failure
     2. Deliberate deletion
     3. Software corruption and viruses

III. Data Recovery
   - A. General Business Matters
   - B. Evidentiary
     1. Protection and Preservation of original data
        - a. Proper storage
        - b. Chain of custody
     2. Expert testimony of recovery technicians
   - C. Recovery
     1. Basic
     2. Advanced

IV. Case Studies

V. Other Considerations
   - A. Recovery from catastrophic physical damage
   - B. Storage, Duplication, Conversion of Outdated Tape Formats
   - C. Trends
   - D. Implications for legal and business
   - E. Advanced Data Recovery Services

VI. Summary

# Advanced Data Recovery and the Legal Profession
# A Continuing Education Course

**A Continuing Education Course**
**TX MCLE Course # 000030851**

## Introduction.

Regardless of specialty, when required an attorney's job may be defined by a single but critical function – gathering, analyzing and presenting evidence. Whether pertaining to civil or criminal law, the basic process is the same – collect pertinent data prepare it according to proper evidentiary rules and present it.

For the past twenty years, and especially with the recent proliferation of the Internet, digital technology has changed greatly. More and more digital data is created, recorded and stored on PCs as well as palm pilots, pagers and mobile phones. These devices are used universally, not only to improve productivity but in every aspect of our personal lives. Consequently, all of these devices are also commonly used to commit crimes and civil wrong doings.

**Figure 1. Typical workstation.**

Digital evidence can be critical to the outcome of legal cases, civil and criminal. Recovery of *digital evidence*, even if assumed to be lost, corrupted or destroyed, can affect legal judgments, and a new set of recovery parameters needs to be understood and applied.

**Figure 2. Open hard drive exposing storage platter.**

When legal or law enforcement investigators must rely on evidence obtained from computers to prove their cases, the method by which digital data *is recovered* can be critical to the outcome of the case.

This course is designed to address one area of ***digital data collection*** and provide an understanding of how data storage works, and how data that is lost, damaged or corrupted and how it can be recovered for use as legal evidence.

This course uses real world cases to provide a foundation with which attorneys might ask appropriate how's, what's and why's when attempting to collect digital evidence. Attorneys will become familiar with the general capabilities of advanced data recovery and the correct legal, physical and evidentiary rules.

## I. Legal considerations in preparation for recovery

**A. General Application.** Data recovery is a process to recover what appears to be lost or irretrievable from electronic media storage devices, BUT IN ALL LIKELIHOOD IS STILL THERE.

Many conventional computer repair services perform relatively simple procedures with off-the-shelf software recovery that essentially can reclaim simple deleted files or repair media sectors or partitions. Firms that advertise a forensics capability also use conventional software recovery procedures that may or may not be targeted to the specific needs of the case. Reliance on either of these levels of recovery alone may result in the potential to miss all of the accessible data that is available for use in a court of law.

It is likely that in 50% of all lost data cases much of the critical data needed to affect a legal outcome is never retrieved. Our experience suggests that most failures occur due to a general lack of understanding about data recovery, even among seasoned computer technologists.

**B. Evidentiary Application.** Hardware and software often fail or are physically damaged; files are routinely, deliberately and accidentally deleted. Many attorneys often conclude (or are counseled to assume) that a loss or corruption of, or damage to, data or storage media is permanent. This is often not the case.

> **"Since 1992 the number of computer crime cases sent to federal prosecutors has tripled, while the number of cases actually prosecuted has remained the same.**
>
> **Of the 419 cases referred to prosecutors, only 83 were prosecuted. The rest were dismissed due to lack of evidence."**
>
> ***Electronic Privacy Information Center (EPIC)***
> ***January 29, 2001***

If an attorney is not aware of some of the advanced data recovery techniques needed to further investigate whether or not files are still present (due to more sophisticated SW or HW tampering), important case data may never be discovered. If a technician performing a recovery is not aware of proper forensics or chain of custody procedures required by the court, no matter how successful the recovery, use of digital evidence may be inadmissible.

When the possibility that digital evidence may have a bearing on a case attorneys need to understand both the limits of the various levels of data recovery, and the methods need to protect and preserve original evidence.

> **Attorneys "need to understand enough about (digital) … technology to ask the right questions and enlist the assistance of the forensic computer experts where necessary.** ***Lawyers who choose to ignore these new opportunities could expose themselves to malpractice claims."***
>
> ***Alan Gahtan***
> ***Brown Raysman, Millstein, Felder & Steiner LLP***

**Imaging and custody chain.** Imaging is used to capture original digital data without changing or writing over it, and creating an exact duplicate of the original drive contents. Since the image is an exact replication of the original, data recovery efforts can be per-

formed on the image and the original drive can be sealed and stored. Knowing how to apply this element of recovery has implications for correct chain of custody. (This is discussed in more detail on page seven.)

## II. Technical Background

**A. How electronic data storage devices work.** Data is generally stored or written, and then accessed or read in one of two ways.

**Magnetic tapes, diskettes hard disk drives** (HDDs) use computer signals to 'rearrange' iron (Fe) oxide properties on coated plastic film.

**Figure 3. Common hard drive devices**

**Figure 4. "Floppy" disks.**

In each case, whether with a hard drive, floppy disk or magnetic tape, data storage is affected by passing an electromagnetic charge onto iron oxide coated plastic. (red lines, Figure 5.)

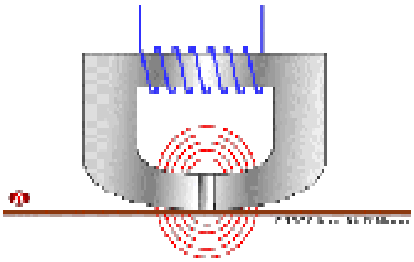
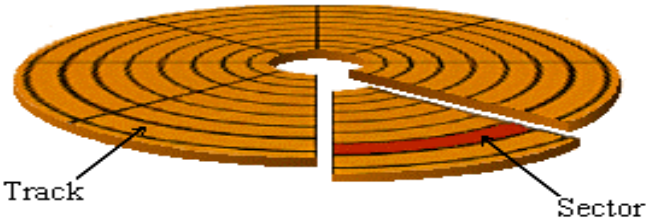


**Figure 5. Electromagnetic current passes over tape or platter.**

A hard drive or diskette platter resembles a vinyl record. It spins, records and accesses data with a device that rides above the disk, just as a record's music "groove" is read with a needle. [1]

Tracks and sectors on the platter physically divide and organize data. A set of instructions on one of the tracks tells the drive how to perform its mechanical functions, i.e. how fast to spin the platter and how to work the electronics


**CDs** Factory programmed plastic CDs, are aluminum-coated disks with impressed microscopic "bumps"; blank CDs uses dye coating instead of aluminum.

[1] The read/write device cannot touch the platter, as this is actually one cause of data failure or crash.

CDs and CD ROMs are molded pieces of clear plastic. On pre-recorded CDs the aluminum-coated plastic is impressed with microscopic "bumps" arranged on a single, continuous (similar to vinyl records), spiral track and layered with aluminum. Microscopic bumps are what the laser reads similar to the way electronically charged oxide is read by magnetic devices.

CD ROMs used for data backup use a dye coating rather than aluminum. As a CD is recorded, the CD "burner" laser heats spots on the dye causing the spots to darken. When reading or retrieving saved data, the laser thinks each "burnt spot" is a bump and reads the data in the same way it would a pre-recorded CD.

**B. Symptoms, causes and types of data failure** There are a variety of common symptoms that indicate data failure has occurred:

- a drive, diskette or tape device appears to be inaccessible,
- a system fails to boot showing a blue screen with unfamiliar instructions,
- an application fails to "open," run correctly, or accept data, or
- a mechanical component fails – failure of the drive to "spin" or clicking sounds.

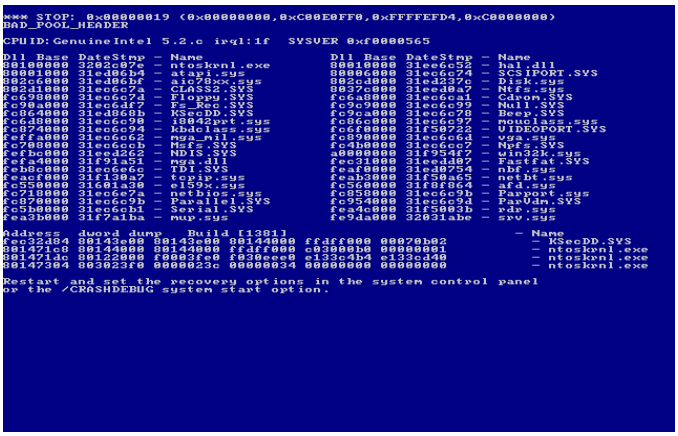



**Figure 6 The "Blue Screen of Death" – indication of serious data or sector damage.**

**Mechanical failure** appears to be the leading cause of data failure. This may occur due to accidents and catastrophic events – such as earthquakes, floods, fire, electrical failure and power surges. Age or abnormal wear (fairly new, well-built systems that sometimes just fail) are among other leading causes of failure.

**Software failure** can occur when there has been improper hardware or software handling or from viruses. This type of failure can occur either by deliberate intent to corrupt or through human error, such as with accidental reformatting or deletion of, or "writing over" of data files.

**Mechanical or software failure** A person intent on doing so, and with the proper knowledge, can induce mechanical or SW failure in order to hide evidence. The truly savvy

user can also replicate any of these symptoms, malfunctions or causes to mask their activities. Certainly arson and other physical misuse can be obvious; however, SW corruption, viruses, the improper loading or use of diagnostic or repair tools are not so obvious. Many times a user will claim files have been "mysteriously erased." It takes a technical specialist to distinguish cause from effect and know how to uncover evidence not readily available from a basic recovery. [2]

In order to affect a successful recovery a technician needs to know how to recognize if and how a system component has failed, or if the file that holds critical data is actually damaged. [3]

## III. Data Recovery

**A. General Business Matters** Computer repair generalists typically use off-the-shelf commercial software that is pre-programmed and able to recover what it is designed to find, such as simple deletes or master file or allocation table corruption. If attempts at recovery are limited to this method with no specific knowledge of what is being sought, suspect data may never be detected.

**B. Evidentiary** Simple and advanced recoveries performed without appropriate procedures may corrupt rules of evidence and render what eventually is recovered as inadmissible.

**Protection and preservation of original data** Computer evidence can be one of the most fragile of legal evidence. In an attempt to recovery data for any application, an incorrect method used to investigate the evidence may in some cases destroy the very information sought. In the case of forensics evidence, even if the data is successfully recovered, inappropriate manipulation, storage and transfer of digital evidence may result in an evidentiary challenge to its authenticity.

**Proper transfer, storage and chain of custody** The generally accepted practice of computer imaging, a non-invasive process to copy an entire media source is a very important step to ensure proper recovery and transfer of evidence. An image file requires very specialized software tools and programming skills to also ensure all information is captured.

**C. Data recovery** and **forensics services** can be classified into three categories of:

- basic recovery
- forensic investigative services
- advanced recovery and litigation support

**1. Basic recovery and forensic services** appear to be a growing industry among providers of general IT services. There are a variety of software packages that are effective in recovering data when a drive partition table, boot record, master file table, FAT or root directory is lost or corrupt. These generally occur when a virus has hit, files are deleted or a drive is formatted or "fdisk'ed" or struck by a power failure. Basic computer foren-

[2] Media device OEMs claim, electronic saves are virtually permanent because the platters and oxides that hold the data are typically warranted for 56 years. The mechanical systems and controllers that 'drive' the storage systems are typically warranted for only 2-3 years. Smart users may know how to induce failure while many others may think they know how but really do not. When building a case an investigator needs to know the difference in the case he or she is pursuing

[3] Think of what would happen if you took a deck of cards and threw them FACE DOWN on the floor. Finding specific cards on the floor without an index is similar to what occurs if computer system tries to find a data file when its filing system is damaged, improperly formatted or erased.

sics services provide more sophisticated software repair and often combine these basic data repairs with proper investigative and evidentiary procedures.

**2. Advanced recovery** services are an investigator's best hope to ensure that every possible measure is taken to retrieve data and protect its integrity in a legal case. There are many SW technicians that know how to affect basic data recovery such as simple deletes, but few experienced, qualified technicians that can provide advanced recovery services.

| Basic Recovery | Forensic Services | Advanced Recovery |
|---|---|---|
| Commercial disk repair software packages | Commercial disk repair and advanced forensic SW | Commercial disk repair, advanced forensic SW and advanced programmer and HW diagnostics services |
| Re-image HDD (*sometimes*) | Re-image HDD | Re-image HDD |
| FAT, master file, directory repair | FAT, master file, directory repair | FAT, master file, directory repair |
| Simple Un-Deletes | Simple Un-Deletes | Simple Un-Deletes |
| | Data Capture | Data Capture |
| | Do not corrupt original drive/data | Do not corrupt original drive/data |
| | Proper Evidentiary Trail | Proper Evidentiary Trail |
| | Investigative expertise, i.e. Fraud, accounting, legal | |
| | Expert testimony – technical and specialized investigative | Expert testimony – technical |
| | Password encryption breaking | Password encryption breaking |
| | | Extensive knowledge of what/where to look; what diagnostics to perform |
| | | **Determine IF a failure is HW or SW related** |
| | | Repair/read severely physically damaged hardware |
| | | Read/format obsolete/ outdated media |

**Table 1. Recovery services comparisons**

In the case of more sophisticated data corruption, it is necessary that a data repair technician have the knowledge of not only basic operating systems and widely used application

software, but also understand the structure of these systems and know how to determine a structure of a privately developed SW package.

Most importantly, many data failures exhibit similar symptoms when caused by either a hardware or software problem. It is important that a recovery technician have the right diagnostics tools to determine the true cause of the failure.

**2. Expert testimony of recovery technicians** Discovery and analysis may have to be performed to provide evidence of culpability, such as matching time and date stamps when data is erased or modified.

| Basic Recovery | Forensics | Advanced Recovery |
|---|---|---|
| Generally not available | Tend to be specific SW experts | Expert in all SW packages |
| | Formal and continuing training | Formal and continuing training |
| | | Expert in non-standard software |
| | | Programming AND engineering backgrounds |
| | | Can go to programming source, rather than rely on interfacing |

**Transfer, storage, chain of custody or conversion from outdated storage media** Correctly recognizing the causes, symptoms and effects of data failure that occur in the general sense is an important part of advanced data recovery. General knowledge of common data failures allows an investigator to decide which type of data recovery is needed and what questions to ask a data recovery expert concerning legal forensics.

## IV. Case Studies

Data recovery for litigation or evidentiary support is a procedure to recovery digital evidence caused by an induced failure and/or an attempt to hide or obfuscate evidence. Depending on severity, loss amount, knowledge of last known backup and criticality, recovery may be affected by transfer or acquisition of damaged or hidden files, or may require an advanced data recovery. Consider the following case studies.

**Case 1. Defendant attempts to induce failure to hide evidence** During divorce proceedings, a wife was suspicious that her spouse may be using a computer for illicit, sexually oriented activities. Believing he could permanently delete the computer evidence of his questionable actions, he reformatted the drive and reloaded the operating system. He then confidently turned the computer over to his wife believing he had 'erased' all of his files permanently. He told his attorney there was no evidence to support his wife's claims.

An advanced data recovery service was able to access the media and reconstruct the 'deleted files' where conventional methods failed.

The advanced recovery technicians "found":

1. pornographic web sites,
2. E-Mail messages to girlfriends, and

3. Outlook calendar appointments made with girlfriends.

All of this evidence was assumed to be non-existent by both the husband and the conventional repair technician who first examined the computer. The recovered files were handed over to the client and her legal counsel. The divorce case was settled in her favor without a trial.

Among the lessons learned by attorney, civil wrong doer and conventional PC technician were that a recovery should not be limited to conventional PC repair methods or PC basic recovery, the technology exists to effectively 'undo' deletes and reformats and an evidence 'paper trail' could be determined.

**Case 2. Attempt to use manipulated electronic evidence to defraud.** A user of a service provider's tracking software pressed a $ 15 MM lawsuit against a Fortune 100 company. Citing negligence plaintiff charged:

1. installation of the software in question had permanently damaged/erased his existing files,
2. the data, most of it irreplaceable, not recoverable by any means, and
3. not only could he not access his irreplaceable data, he could not access what files were left in a specific software application critical to running his business.

Concerned the company might in fact be liable, chief counsel with advice from the company's IT director considered settling with the plaintiff and doing a complete review or re-write of the company's software.

Before making a final decision, the company attorney decided to try an advanced data recovery service to determine if his company was liable or if that liability could be mitigated. This "last resort" process had multiple and unexpected positive outcomes for the company.

The first phase of the recovery was able to accurately restore all of the "lost" files and allowed the dismissal of the 2nd charge – the data was unrecoverable.

During a second more advanced phase, programmers were able to restructure and reformat files needed for the claimant's specific software application. The advanced data recovery team was able to reprogram this data when the simple data recovery was not successful, dismissing liability for the 3rd charge – the data once repaired could not be used in a specific software package for the plaintiff to use to run his business.

The third phase of advanced forensic analysis, using electronic data discovery, forensic and analysis applications revealed that the SW installation had nothing to do with the lost data (further rejecting the 1st charge), and determined the plaintiff had manually erased the alleged lost data.

The plaintiff dropped his case and the defendant could have pursued criminal charges against their accuser but settled for an out-of-court settlement to cover legal and data recovery costs.

**Case 3. Attempt to hide the theft of proprietary software.** A programmer and security expert with ten years experience was hired to develop a company's proprietary software. Eventually, the employee decided to leave the company, but first he made copies of all the relevant files for his own use and deleted all the matching corporate data files. The disgruntled employee first made copies to his laptop, then copied those files to an-

other computer and reformatted the hard drives of his work station, the company server and his laptop, and finally he installed a new operating system on the laptop and the work station.

An advanced data recovery team reviewed and copied an exact image of the company drive, un-deleted the critical files from the image and established an exact deletion date and time. (Deletion date and time matched defendant's "log-in" to his PC and the system server and access to physical facility via his door-access code.)

During depositions, the recovery experts were challenged by the defendant's attorney (the defendant claiming himself to be an expert IT witness) that data of this type "was impossible to recover." During the challenge, the recovery experts were able to prove to both the litigants and the judge that not only was it possible they had proof of the recovery and they could trace the data deletions specifically to the defendant.

The defendant accepted a $40 K judgment against him rather than go to trial. Not only was the plaintiff company able to recover its valuable SW, they were able to use the intentional deletions as evidence against the defendant.

## V. Other Considerations

**A. Recovery from catastrophic physical damage** Whether by accident or with intent, there are cases where plane crashes, fire, arson or floods damage systems which seem to make recovery of electronic evidence impossible. It is important to remember that as long as the platters that hold electronically charged oxides on magnetic media, or 'bumps' and 'dye marks' on CDs are not damaged, there is a good chance that all or some of the data can be recovered.

The figure on the right is an illustration of one of five fire-damaged UNIX server drives literally shoveled out of the debris from large auto dealership.

Since the (plastic-material) backup tapes had been co-located with the server drives and were themselves destroyed, all financial data – inventory, accounts payable and receivable, W-2s, customers and loan information – was destroyed.

Nearly 100% of data from these drives were recovered within three days.

**Figure 7. Fire damaged UNIX drive.**

Had the recovery failed, implications from downtime, potential business or insurance fraud could have been astronomical.

**B. Storage, duplication and conversion of media from outdated tape formats** Improvements in PCs, the explosion of the use of MS Windows and the Y2K phenomena have caused many large data users to move from mainframe to PCs and servers very quickly. Today, litigants may need data:

- that has been stored on "old" mainframe backup tape systems,
- was never converted, and
- was either damaged or supported only by obsolete or unavailable operating systems.

In a recent criminal negligence case a data recovery service was able to successfully recover data from just such an old system.

Three years previous, a truck owned by the plaintiff had hit a car and killed three individuals. The plaintiff's trucking firm had been recording raw data on all vehicle travel tracked with GPS but had saved it on an old "main-frame" computer fed by (now outdated) 9-track data tapes. (The mainframe had been upgraded in 1999 since it was not Y2K compliant.)Data recovery experts were able to isolate from the records of approximately 350 trucks over a 10-year period and the driver in question's travel records over a two-year period, and translate the data to a PC readable format.

In the discovery, acquisition and analysis phases the recovery experts were able to validate the data in question under deposition. Evidence was located and read from tapes that were more than 10 years old and were provided to both sides' attorneys. Both plaintiff and defendant were so satisfied with the data that the case was settled out of court.

Chain of custody. Immediate access to the evidence was provided to both sides of the case and was certified for use as evidence if court proceedings were needed. While the data was being recovered, strict control of the tapes and drives was needed.

**Trends** As with many businesses today the trend in developing storage is to do more with less. The computer, recent great strides in personal and enterprise software and the incredible capability and autonomy that all professions have experienced with new technologies have been a leading factor driving new storage trends.

Growth in the complexity and miniaturization of storage devices will be a large part of this continuing trend. Twenty years ago the amount of data that could be stored on a drive the size of a TV set can now be stored on a small laptop drive. Five years ago, what could be stored on a desktop drive is about one-third of what can be stored on today's laptop drive. In less than five years, most desktop drives will be as small as today's laptop drives and possibly hold two to three times as much data, and what today's small laptop drives hold will fit on a device the size of a key ring.

Another trend is growth in medium and large sized HDD systems. International Data Corporation (IDS) forecast the market growth from 1999 to 2005 would see a doubling of enterprise and medium-size computer system HDD growth – from approximately $3.5 – $4 B in 1999 to $7 B in EACH class, much of this growth from devices smaller than today's 3.5" drives.

The recent growth in smaller and more capable devices is accompanied by a rapid growth in problems related to improper storage, failed (or a lack of proper) backups and fraudulently damaged or obfuscated files.

**C. Implications for legal and business** So far we have discussed recovery and its direct implications for the legal community vis-à-vis litigation and support. It would be helpful to consider that in one area – civil or criminal litigation in business cases – the cost of damaged or lost data can be severe.

When involved in cases involving criminal or civil negligence, it is important to have an understanding of the scope of losses that can be directly attributable to the data loss itself. There are over 20 business categories that have been identified as subject to <u>severe</u> business losses when data that drives their mission critical processes has been lost.

The following table lists the PER HOUR cost of downtime by industry.

| Industry Type | Revenue/ Hr ($000s) | Revenue/ Employee |
|---|---|---|
| Energy | 2,817 | 569 |
| Telecommunications | 2,066 | 187 |
| Manufacturing | 1,610 | 134 |
| Financial Institutions | 1,495 | 1,080 |
| Information Technology | 1,344 | 184 |
| Insurance | 1,202 | 371 |
| Retail | 1,107 | 244 |
| Pharmaceuticals | 1,082 | 168 |
| Banking | 997 | 131 |
| Food/beverage processing | 804 | 153 |
| Consumer products | 785 | 128 |
| Chemicals | 704 | 195 |
| Transportation | 669 | 108 |
| Utilities | 643 | 381 |
| Health Care | 636 | 143 |
| Metals/natural resources | 581 | 153 |
| Professional Services | 533 | 100 |
| Electronics | 477 | 75 |
| Construction and engineering | 341 | 216 |
| Media | 331 | 120 |
| Hospitality & Travel | 330 | 330 |
| Average | 979 | 246 |
| Median | 785 | 168 |

**Table 1. The cost of downtime by industry**

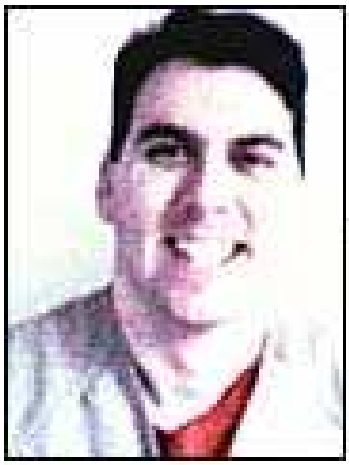
*Source: IT Performance Engineering & Measurement Strategies Oct 2000*

The most important aspect of this section is to realize that data failure occurs often, most times without warning and often times the cost of recovery is more economical than continued downtime.

The recent sentencing of David Smith, author of the 'Melissa' virus, to 20 months has brought this issue to light.

It is estimated that Melissa cost business more than $80 MM in downtime. If one accepts the estimates of researchers that more than half of potential recoveries are not performed, it could be argued that in this case, business losses of $40 MM might have been mitigated if advanced recovery technology were better known.

Many experts claim this is only the beginning of this type of "white collar" sabotage." *(AP, 2002)*



**Convicted: David Smith**

**D. Advanced Data Recovery.** Whether by accident or intent, damage to physical systems can occur that would make investigation of electronic data evidence appear impossible.

It is important to remember that if the platters that hold electronically charged oxides on magnetic disks or tapes, or the CDs that hold "bumps" and "dye marks" are not too damaged, there is a good chance that all or much of the data, hitherto thought to be lost, can be recovered.

There are really only a few highly trained specialists able to perform data recovery and forensics with any level of confidence. And while basic recovery can simple deleted or "lost" files, advanced recovery and proper evidentiary procedures are often needed to advance a case.

Advanced data recovery utilizes the ability to recover data with knowledge of how chain of custody and data contamination procedures effect digital evidence preparation. Computer forensics experts look at *available* digital files with an accountant's, environmentalist's or architect's trained eye, and see information that is incorrect, where mistakes have been made and where information has purposely been falsified.

Consider Al Capone's tax evasion trial – forensic experts looked at his books (both sets of them) to find a money trail to determine that Capone really made more than the $2000 a year he claimed. An advanced data forensic recovery expert, would be able to find the books at the bottom of a river and make them legible, and would be able to show where Capone's accountant erased and replaced certain figures in the ledgers.

Most firms recognized as computer or digital forensic professionals perform simple data retrievals, un-deletes, directory repairs and re-imaging of electronic media. The advanced recovery process goes beyond that to find data likely to be missed using simple recovery and forensics methods.

***Checklist.*** The following is a checklist an investigator might want to consider when developing a case with digital evidence:

Are the services being used to gather electronic evidence exploit:

- a capability to rebuild a damaged media device, such as in a "clean room," and
- large storage capacity for duplication, imaging and conversion of media from outdated to newer or advanced formats?

Can the forensic and programming procedures being used withstand chain of custody or evidential integrity challenges posed in court? Do the experts being used have experience with many types of operations, hardware and file systems and media storage devices:

- Tapes – cassettes, drives -- HDDs, diskettes, CDs and other emerging optical systems
- PCs laptops, servers
- MS/DOS, Macintosh, UNIX, Linux

Because permanent loss of data could occur and have severe consequences a good data recovery specialist should provide timely response with the proper solution. A full service data recovery and forensics services firm knows how to:

- Image the electronic media
- Repair the electronic allocation (FAT) file or tape catalogue
- Discern specifics of a FAT or catalogue damage
- Identify if a file or a FAT has been fragmented
- Physically rebuild a hard drive to get it to spin and access data.

## VI. Summary

Many, who deliberately tamper with data or, try to make it appear that the data has been inadvertently damaged or lost, are relying on the theory that either computer data is permanently "lost" or the false perception that if recovered, data cannot be traceable back to them or their nefarious activities

At the heart of computer forensics recovery are the correct techniques used to retrieve information from electronic systems that:

- can stand the test of evidence,
- may appear to an investigator to be permanently lost or damaged, but is actually still on the media device, and
- may be permanently lost if attempted with the wrong techniques.

A litigant having the basic knowledge of data recovery and forensics, and having an advanced data recovery provider can mean the difference between winning and losing. It may also mean failing to prosecute or defend to the limits of today's technology capability.

Despite the fact that disaster data recovery appears to be of growing concern, there are still only about five companies nationwide that have the experience, the personnel and the capital equipment to do a credible job.

The oldest and the largest advanced data recovery firms are listed below:

| **The oldest** | **The largest** |
|---|---|
| **Data Recovery Services, Inc** | **OnTrack** |
| 2636 Walnut Hill Ln Suite 230 | 9023 Columbine Rd |
| Dallas, TX 75229 | Eden Prairie, MN 55347 |
| 214 350-8202 | 952 937-5161 |
| 877 304 7189 (toll free) | 952 937-5750 |
| www.datarecovery.net | www.ontrack.com |

**About the presenter/author.**

Thomas J Kapurch is a former Intelligence Officer, US Navy and Defense Intelligence Agency, with more than 15 years experience in information systems, intelligence collections, analysis, technical information systems, geo-political intelligence and military investigations.

His industry experience includes over ten years in business and information systems management for GTE, Nextel, NEC America, TXU, Informatica Software Company with 11 years experience developing business and operations plans, as internal and external information systems consultant to telecommunications, utilities and financial companies.

Mr. Kapurch worked as an engineer with Texas Instruments on computer based aerospace products with OEMs and major subcontractors Bell Textron, McDonnell Douglas, Boeing and Lockheed. While at TI, Kapurch also managed all phases of electronics systems and components manufacturing and enterprise wide information systems for manufacturing and shipping.

He is currently Vice-President of Data Recovery Services Inc. in Dallas, Texas, responsible for designing and presenting technology seminars for litigation support and government services.

**Education**

| | |
|---|---|
| BS, Engineering, US Naval Academy, Annapolis, MD | 1975 |
| MBA, University of Dallas, Irving, TX | 1988 |
| MA, Strategic Studies, US Naval War College | 1991 |
| MA, International Relations and Politics | 1991 |

# Appendix A

## e-Evidence and Discovery in Legal Decisions

### e-Evidence and Discovery Relevance

***Rowe Entertainment, Inc. v The William Morris Agency***, 2002 WL 975713 (SDNY 9 May 2002). "Rules 26(b) and 34 for the Federal Rules of Civil Procedure instruct that computer-stored information is discoverable under the same rules that pertain to tangible, written materials."

***Rowe Entertainment, Inc. v The William Morris Agency***, 2002 WL 63190 (SDNY 16 Jan 16 @002). Denying Defendants' motion for a protective order insofar as it sought to preclude the discovery of email altogether, the Court adopted a balancing approach, consisting of eight factors, to determine whether discovery costs should be shifted.

After reanalyzing and reaffirming the 8 factor balancing test, the Court upheld the 15 Jan 2002 Order that granted Defendants motion to shift the costs of production of their e-mail communications to Plaintiffs.

***Crown Life Ins. Co. v Craig*****,** 995 F.2d 1376 (7th Cir. 1993). Computer data is discoverable under Federal Rule of Procedure 34.

***Anti-Monopoly, Inc. v Hasbro, Inc.*****,** 1995 WL 649934 (SD NY 3 Nov 1995). "The law is clear that data in computerized form is discoverable even if paper 'hard copies' of the information have been produced…[T]oday it is black letter law that computerized data is discoverable if relevant."

***Stallings-Daniel v Northern Trust Co*****.,** 2002 WL 385566 (ND IL 12 Mar 2002). In an employment discrimination action, the Plaintiff moved for reconsideration of the Court's denial of electronic discovery of the Defendant's email system. The court, in denying the Plaintiff's motion for reconsideration, determined the ***Plaintiff presented no new information that justified an intrusive electronic investigation***.

***Storch v IPCO Safety Prods. Co****.,* 1997 WL 401589 (ED PA 16 July 1997). "This Court finds that in this age of high-technology where much of our information is transmitted by computer and computer disks, it is not unreasonable for the defendant to produce the information on computer disk for the plaintiff."

***Guillen v Pierce County,*** 31 P3d 628 (WA 13 Sep 2001). Widower filed complaint under Public Disclosure Act (PDA), seeking access to historical accident reports (for use in connection with a pending tort case) held by county agencies, relating to the traffic intersection at which his wife was killed. The Court held that the PDA provision generally prohibiting accident reports (including electronic reports and databases) prepared by people involved in accidents from being used as evidence in any civil or criminal trial ***does not preclude pretrial discovery of such reports***. Notably, the Court stated, "As governments everywhere move from paper and microfiche documentation into the age of 21st Century information technology, public records are increasingly being stored and created in digital format, then added to virtual databases that are accessed, in streams of bits and bytes, by vast networks of governmental agencies, often across jurisdictional boundaries…"

***McPeek v Ashcroft*****,** 202 FRD 31 (DDC 1 August 2001). "... economic considerations have to be pertinent if the court is to remain faithful to its responsibility to prevent 'undue burden or expense'...If the likelihood of finding something was the only criterion, there is a risk that someone will have to spend hundreds of thousands of dollars to produce a single e-mail. That is an awfully expensive needle to justify searching a haystack."

***Benton v Allstate Ins. Co****.,* 2001 WL 210685 (CD CA 26 Feb 2001). The court refused to grant a continuance on defendant's summary judgment motion where plaintiff claimed that he had not had an adequate opportunity to conduct discovery of defendant's computer system. The court concluded that the plaintiff did not show that a further continuance was necessary to prevent irreparable harm or that further discovery will enable him to obtain evidence essential to his opposition to the motion.

***Columbia Communications v Echostar***, 2 Fed.Appx. 360 (4th Cir 2001). In a contract dispute, the Court held that failure of the lessor to turn over certain computer databases during discovery did not justify a judgment for the distributor or a new trial.

***White v White***, 781 A.2d 85 (NJ Super. Ct Ch Div 2001). In a divorce action, the husband filed a motion to suppress his e-mail that had been stored on the hard drive of the family computer. The Court held that

the wife did not unlawfully access stored electronic communications in violation of the New Jersey Wiretap Act and did not intrude on his seclusion by accessing those e-mails. "Having a legitimate reason for being in the files, plaintiff had a right to seize evidence she believed indicated her husband was being unfaithful….Is rummaging through files in a computer hard drive any different than rummaging through files in an unlocked file cabinet…Not really."

***Byrne v Byrne,*** 650 N.Y.S.2d 499 (NY Sup Ct 1996). In a divorce proceeding, the wife sought access to her husband's computer, which husband used for both business and personal purposes even though computer was provided by husband's employer. The wife was awarded such access to search the computer for information about the couple's finances and marital assets.

***Linnen v A.H. Robins Co.,*** 1999 WL 462015 (MA Super. 16 Jun 1999). "A discovery request aimed at the production of records retained in some electronic form is no different in principle, from a request for documents contained in any office file cabinet." The court continued, "To permit a corporation such as Wyeth to reap the business benefits of such [computer] technology and simultaneously use that technology as a shield in litigation would lead to incongruous and unfair results."

***Strasser v Yalamanchi***, 669 So.2d 1142 (Fla. Dist. Ct. App. 1996). The court ruled that the trial court's discovery order should be quashed because (1) unrestricted access to Defendant's entire computer system was overly broad and would pose a threat to confidential records and (2) there was little evidence that the purged documents could be retrieved.

***Fennell v First Step Designs, Ltd.***, 83 F.3d 526 (1st Cir 1996). The court denied Plaintiff's broad request for discovery of Defendant's entire hard drive. The court explained that the costs, burdens, delays, and likelihood of discovering the evidence must be weighed against the importance of the requested evidence. Court held requesting party must show a "particularized likelihood of discovering appropriate material".

***Murlas Living Trust v Mobil Oil Corp.*,** 1995 WL 124186 (ND IL 20 Mar 1995). The court refused to require Defendant to undergo intrusive or burdensome discovery for its electronic files where the burden is not justified by the relevance of the evidence likely to be discovered.

***Easley, McCaleb & Assoc., Inc. v Perry*,** No. E-2663 (GA Super Ct 16 Jul 1994). Court ordered that deleted files on Defendant's computer hard drive are discoverable, and Plaintiff's expert must be allowed to retrieve all recoverable files. Court issued an order detailing the protocol for reviewing the electronic data.

***PHE, Inc. v Department of Justice***, 139 FRD. 249 (DDC 1991). Court ordered Plaintiffs to produce computerized tax records even though Plaintiffs possessed no computer program to retrieve or display the records. "Although no program may presently exist to obtain the information requested, the Court is satisfied that with little effort the plaintiffs can retrieve the necessary and appropriate information…It would not be unreasonable to require the plaintiffs to incur modest additional expenditures so as to provide the defendants with the discovery necessary to establish that they are not acting in bad faith and vindictively."

## e-Evidence and Discovery Cost

***In re Air Crash Disaster at Detroit Metro*,** 130 FRD. 634 (ED MI 1989). In litigation brought after a passenger jet crash, the court ordered the aircraft manufacturer to provide relevant flight simulation data on computer-readable nine-track magnetic tape even though the aircraft manufacturer had already provided the data in hard copy print-outs. Because material did not currently exist on magnetic tape, the requesting party (the airline) was required to pay all and necessary costs associated with manufacture of tape.

***Williams v Saint-Gobain Corp***., 2002 WL 1477618 (WDNY. 28 Jun 2002). In an employment discrimination suit, the Court refused to issue sanctions or attorney's fees stemming from myriad discovery disputes. Despite an earlier assertion that no further responsive documents could be located, the Defendant produced emails obtained from an executive's computer five days before trial. Many other messages were deemed irretrievable, due to changes in the company's email system prior to litigation. Because the messages were found in another form, the Court set aside the interesting question of whether it was appropriate for the company to switch systems in a way that rendered old email irretrievable. In denying Plaintiff's motion for sanctions, including an adverse inference, the Court found no evidence of any bad faith as to the withholding or destruction of the emails and issued the parties an extended time period to complete discovery. As part of the extended discovery, the Court ordered the Defendant to make the CD-ROM of

the executive's hard drive (from which the email was retrieved) available for inspection by the Plaintiff. The Court ordered each party to bear its own discovery costs.

***Van Westrienen v Americontinental Collection Corp.,*** 189 FRD 440 (D OR 1999). Court held that "Plaintiffs are not entitled to unbridled access [of] Defendant's computer system…Plaintiffs should pursue other less burdensome alternatives, such as identifying the number of letters and their content."

***Toledo Fair Hous. Ctr. v Nationwide Mut. Ins. Co.,*** 703 N.E.2d 340 (OH CP 1996). The court ordered discovery of certain documents from Defendant's database. Judge stated that the Defendant cannot avoid discovery simply because their own record keeping scheme makes discovery burdensome. Court ordered Defendant to pay costs of the discovery

***Rhone-Poulenc Rorer, Inc. v Home Indemnity Co.,*** 1991 WL 111040 (ED PA 17 Jun 1991). An unwieldy computerized record-keeping system, which requires heavy expenditures in money and time to produce relevant records, is simply not an adequate excuse to frustrate discovery. Plaintiffs were required to pay for copies of any documents on microfilm/microfiche which Plaintiff requests, while Defendants bear the burden of searching and producing the documents.

## e-Evidence and Discovery Procedure

***Ingenix, Inc. v Lagalante*****,** 2002 U.S. Dist. LEXIS 5795 (ED LA. 28 Mar 2002). Defendant left his employment with the Plaintiff to work for Plaintiff's competitor, as a VP of sales. The Plaintiff (Defendant's former employer) filed suit against Defendant alleging fraudulent, abusive, and knowing misappropriation of computer files and proprietary information causing damage in excess of $5,000 in violation of the Computer Fraud and Abuse Act. While the CFAA is a criminal statute, the court affirmed the rule that a violation of the statute can provide the basis for civil liability. Plaintiff's allegations were based upon evidence that the Defendant had misused his company laptop and took steps to appropriate data relating to customers "in the sales funnel" for his new employer. A computer forensic examination of email messages sent by Defendant and the pattern of Defendant's use and downloading of files from his laptop revealed that he had, in fact, downloaded and deleted confidential and proprietary customer information for use by Plaintiff's competitor.

***Murphy Oil USA, Inc. v Fluor Daniel, Inc.***, 2002 WL 246439 (ED LA 19 Feb 2002). The Court used the eight-factor balancing test set forth in ***Rowe*** to determine operating protocols and the cost shifting formula. It placed the burden on the producing party to elect one of two proposed protocols.

***Rowe Entertainment, Inc. v The William Morris Agency***, 205 FRD. 421 (SDNY 2002). Denying Defendants' motion for a protective order insofar as it sought to preclude the discovery of email altogether, the Court set forth an eight factor balancing test for identifying responsive emails while protecting privileged documents. *See also Rowe Entertainment, Inc. v The William Morris Agency*, 2002 WL 975713 (S.D.N.Y. May 9, 2002). After reanalyzing and reaffirming Judge Francis' eight factor balancing test, the Court upheld the January 15, 2002 Order that granted Defendants motion to shift the costs of production of their e-mail communications to Plaintiffs.

***McPeek v Ashcroft*****,** 202 FRD 31 (DDC 1 August 2001). In a sexual harassment action against Plaintiff's employer, Plaintiff sought to force Defendant to search its backup systems for data that was deleted by the user but was stored on backup tape. Defendant rebutted that the remote possibility of yielding relevant evidence could not justify the costs involved. Instead of ordering recovery and production of relevant documents from all of the existing backup tapes, the Magistrate ordered the Defendant to restore and produce responsive emails from one person's computer over a one year period. After this sample data was produced and accessed, the Magistrate would then determine if a broader recovery and search was warranted given the burden and expense.

***Carbon Dioxide Indus. Antitrust Litig.*****,** 155 FRD. 209 (MD FL 1993). "[D]epositions to identify how data is maintained and to determine what hardware and software is necessary to access the information are preliminary depositions necessary to proceed with merits discovery."

## Preservation of e-Evidence

***Heveafil Sdn. Bhd. v United States*****,** 2001 WL 194986 (Ct Int'l Trade 27 Feb 2001). In an action challenging a US Department of Commerce administrative review of an "antidumping order", the court determined the plaintiff failed to act to the best of its ability where six months after receiving notice about maintaining its source documents, it deleted relevant data from its computer system. The court found that the plaintiff "did not cooperate to the best of its ability because after receiving notice from [the Department of Commerce], it knew or should have known to maintain th[is] source document."

***Adobe Sys., Inc. v Sun South Prod., Inc.,*** 187 F.R.D. 636 (SD CA 1999). In a computer piracy suit, the Court denied Plaintiff's *ex parte* application for a temporary restraining order. The Court based its decision on the fact that it is more difficult to erase evidence that is magnetically encoded on a computer hard disk than it is to physically destroy floppy disks, compact discs, invoices, and other tangible forms of evidence. "Manual or automated deletion of that software may remove superficial indicia, such as its icons or presence in the user's application menu. However, telltale traces of a previous installation remain, such as abandoned subdirectories, libraries, information in system files, and registry keys…Even if an infringer managed to delete every file associated with Plaintiffs' software, Plaintiffs could still recover many of those files since the operating system does not actually *erase* the files, but merely marks the space consumed by the files as free for use by other files."

***Linnen v A.H. Robins Co.,*** 1999 WL 462015 (MA Super 19 Jun 1999). Defendant Wyeth failed to preserve emails and neglected turning over database information ordered by the court. The court sanctioned Wyeth for such "inexcusable conduct" and allowed spoliation inference to be given to jury.

***Lauren Corp. v Century Geophysical Corp*****.,** 953 P.2d 200 (CO Ct App 1998). In a breach of licensing agreement suit, Defendant's employees, with knowledge of the significance of the hardware as crucial evidence in the lawsuit, destroyed computer hardware. Appellate Court held that a trial court may impose attorney fees and costs as a sanction for the bad faith and willful destruction of evidence, even in the absence of a specific discovery order.

## e-Evidence and Discovery in Criminal Cases

***United States v Tucker***, 150 F.Supp.2d 1263 (D. UT 2001). The Defendant was found guilty of knowing possession of child pornography. The conviction was largely supported by computer forensic evidence found in the form of deleted Internet cache files that were saved to the Defendant's hard drive when he viewed the various websites.

***State v Guthrie***, 627 N.W.2d 401 (SD 2001). In a criminal prosecution for murder, a computer specialist conducted several forensic searches on a computer used by the Defendant, finding that the computer had been used to conduct numerous Internet searches on subjects related to the incidents surrounding the murder. In addition, the forensic analysis was able to reveal that a computer printed suicide note, offered to exculpate the Defendant, was created several months after the victim's death.

***Demelash v Ross Stores, Inc****.,* 20 P.3d 447 (WA Ct. App 2001). In an action for a false shoplifting arrest, the court stated, "A trial court must manage the discovery process in a fashion that promotes full disclosure of relevant information while at the same time protecting against harmful side effects. Consequently, a court may appropriately limit discovery to protect against requests that are unduly burdensome or expensive." The court limited the scope of to a computerized summary of the store's files.

***Broderick v State***, 35 S.W.3d 67 (TX App 2000). In child sex abuse prosecution, the court affirmed the trial court's admission of a duplicate of defendant's hard drive, in place of the original. The court concluded that the state's best evidence rule did not preclude admission because the computer expert testified that the copy of the hard drive exactly duplicated the contents of the hard drive.

## e-Evidence and Discovery in Corporate Cases

***RKI, Inc. v Grimes***, 177 F.Supp.2d 859 (ND IL 2001). In a trade secret misappropriation action against Plaintiff's former employee, the Court found that the Defendant de-fragmented his home computer in an effort to prevent plaintiff from learning that he had deleted confidential information and software. The Court ordered the Defendant to pay $100,000 in compensatory damages, $150,000 in punitive damages, attorneys' fees, and court costs.

***Minnesota Mining & Mfg. v Pribyl***, 259 F.3d 587, (7th Cir. 2001). Plaintiff brought suit against three former employees for misappropriation of trade secrets. The appellate court affirmed the trial court's negative inference instruction to the jury where the one Defendant committed spoliation of evidence by downloading six gigabytes of music onto his laptop, which destroyed many files sought by the Plaintiff, the night before Defendant was to turn over his computer pursuant to the discovery request. However, the fact that hard drive space was destroyed on one Defendant's computer did not relieve the Plaintiff from proving the elements of its claims.

***Trigon Ins. Co. v United States***, 2001 WL 1456388 (E.D.Va. Nov. 9, 2001). Based on computer forensic expert analysis, the Court found that the Defendant willfully and intentionally destroyed documents that should have been produced during discovery. The Court issued adverse inferences and reimbursement of Plaintiff's attorneys fees as damages for the spoliation.

***Illinois Tool Works, Inc. v Metro Mark Prod. Ltd.***, 43 F.Supp.2d 951 (N.D. Ill. 1999). In an unfair competition case, the court ordered the Defendant to produce for inspection its computer after Plaintiff showed that the Defendant had been less than forthcoming in producing hard copies of requested documents. The court further issued sanctions, in the form reasonable attorney's fees and costs, for the failure to comply with the discovery orders.

***Illinois Tool Works, Inc. v Metro Mark Prod., Ltd.,*** 43 F.Supp.2d. 951 (N.D. Ill. 1999). The court held that sanctions, in the form of attorney's fees and additional discovery costs, against the Defendant were warranted as a remedy for spoliation.

***United States v Koch Ind.,*** 197 F.R.D. 463 (N.D. Okla. 1998). Plaintiffs claimed that Defendant thwarted discovery attempts by destroying backup computer tapes and files. Court found that Defendant failed in its duty to preserve evidence that it should have known was relevant. Court allowed Plaintiffs to inform jury that computer tapes and files were destroyed but did not allow negative inference.

***New York State NOW v Cuomo***, 1998 WL 395320 (S.D.N.Y. July 14, 1998). The court refused to impose sanctions on Defendants for destroying computer databases where there was no showing that the Defendants deleted computer databases or destroyed monthly summary reports in order to impede litigation and the plaintiffs failed to demonstrate that they were prejudiced by the loss of the records.

***Computer Assocs. Int'l, Inc. v American Fundware, Inc***., 133 F.R.D. 166 (D. Colo. 1990). Court issued a default judgment were Defendant revised portions of the source code after being served in the action, and thus put on notice that the source code was irreplaceable evidence. Revised code was a central piece of evidence to the litigation.

## e-Evidence and Discovery Regarding the Use of a Neutral Expert

***Munshani v Signal Lake Venture Fund II*****,** 2001 WL 1526954 (MA.Super. Oct. 9, 2001). In a dispute over authentication of an email message, the Court appointed a neutral computer forensics expert. Based on the expert's analysis and report, the Court found that the Plaintiff intentionally fabricated the disputed email and then attempted to hide that fabrication. The Court dismissed the Plaintiff's suit and ordered him to pay the Defendant's expert and attorney fees.

***Northwest Airlines v Local 2000***, CA No 00-08DWF/AJB (D MN 2 Feb 2000) (Order on Defendants' Motion for Protective Order and Plaintiff's Motion to Compel Discovery); (Memorandum Opinion and Order). Court ordered Plaintiff's expert to act as a neutral 3rd party expert; on behalf of the court, the expert collected and imaged the Defendants' personal hard drives and provided the parties with a complete report of all data "deemed responsive." Court issued detailed protocol for conducting the electronic discovery.

***Simon Property Group v mySimon, Inc.,*** 194 FRD 639 (SD IN 2000). On Plaintiff's motion to compel in a trademark case, the court held that Plaintiff was entitled to attempt to recover deleted computer files from computers used by Defendant's employees. The court required that protective measures be taken, including Plaintiff's appointment of an expert who would serve as an officer of the court and turn over the recovered information to Defendant's counsel for appropriate review.